Error de Aborto de TLS del módulo de servicios NGFW debido a error de intercambio de señales o de validación de certificado

Contenido

Introducción

Este documento describe cómo resolver un problema particular con el acceso a sitios web basados en HTTPS a través del módulo de servicios de firewall de última generación (NGFW) de Cisco con el descifrado habilitado.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Procedimientos de entrada en contacto de capa de conexión segura (SSL)
- Certificados SSL

Componentes Utilizados

La información de este documento se basa en el módulo de servicios de Cisco NGFW con Cisco Prime Security Manager (PRSM) versión 9.2.1.2(52).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

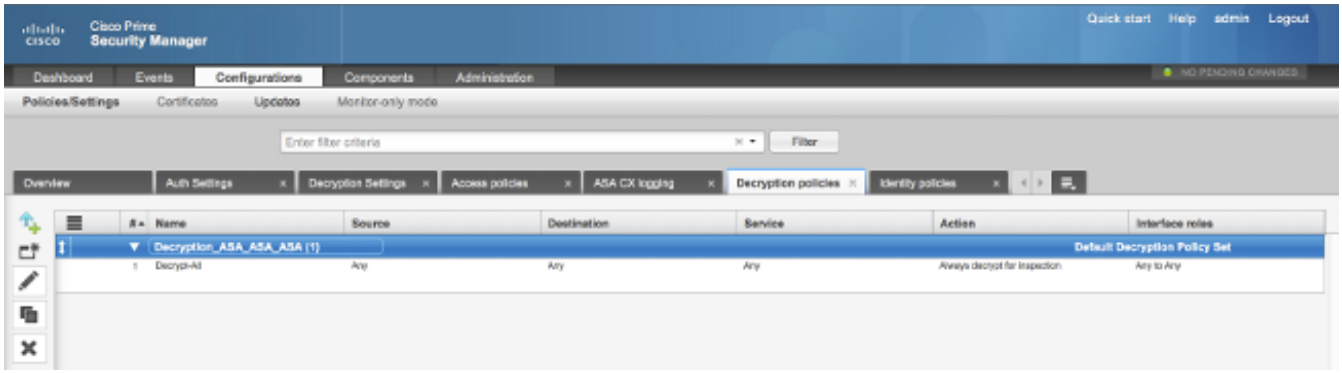
Antecedentes

El descifrado es una función que permite al módulo de servicios de NGFW descifrar flujos cifrados por SSL (e inspeccionar la conversación que se cifraría de otro modo) y aplicar políticas en el tráfico. Para configurar esta función, los administradores deben configurar un certificado de descifrado en el módulo NGFW, que se presenta a los sitios web basados en HTTPS de acceso del cliente en lugar del certificado del servidor original.

Para que el descifrado funcione, el módulo NGFW debe confiar en el certificado presentado por el servidor. Este documento explica las situaciones en las que el intercambio de señales SSL falla entre el módulo de servicios NGFW y el servidor, lo que hace que ciertos sitios web basados en HTTPS fallen cuando intenta alcanzarlos.

A los efectos de este documento, estas políticas se definen en el módulo de servicios NGFW con PRSM:

- **Políticas de identidad**: No hay políticas de identidad definidas.
- **Políticas de descifrado**: La política **Descifrar todo** utiliza esta configuración:

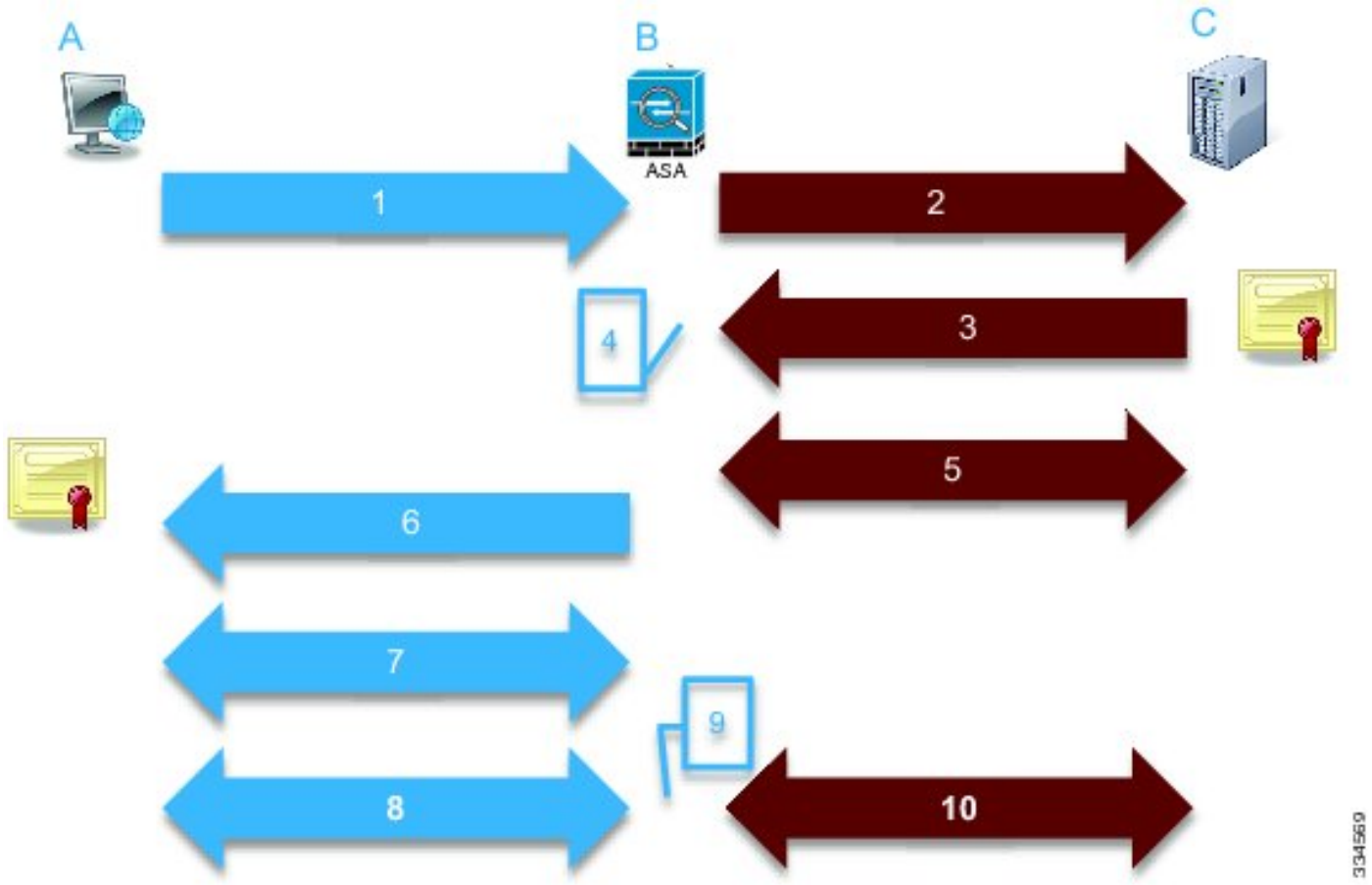


- **Políticas de acceso**: No hay políticas de acceso definidas.
- **Configuración de descifrado**: Este documento asume que un **certificado de descifrado** se configura en el módulo de servicios de NGFW y que los clientes confían en él.

Cuando se define una política de descifrado en el módulo de servicios de NGFW y se configura como se describió anteriormente, el módulo de servicios de NGFW intenta interceptar todo el tráfico cifrado SSL a través del módulo y el descifrado.

> **Nota:** Una explicación paso a paso de este proceso está disponible en la sección Descifrado del Flujo de Tráfico de la Guía del Usuario para ASA CX y Cisco Prime Security Manager 9.2.

Esta imagen representa la secuencia de eventos:



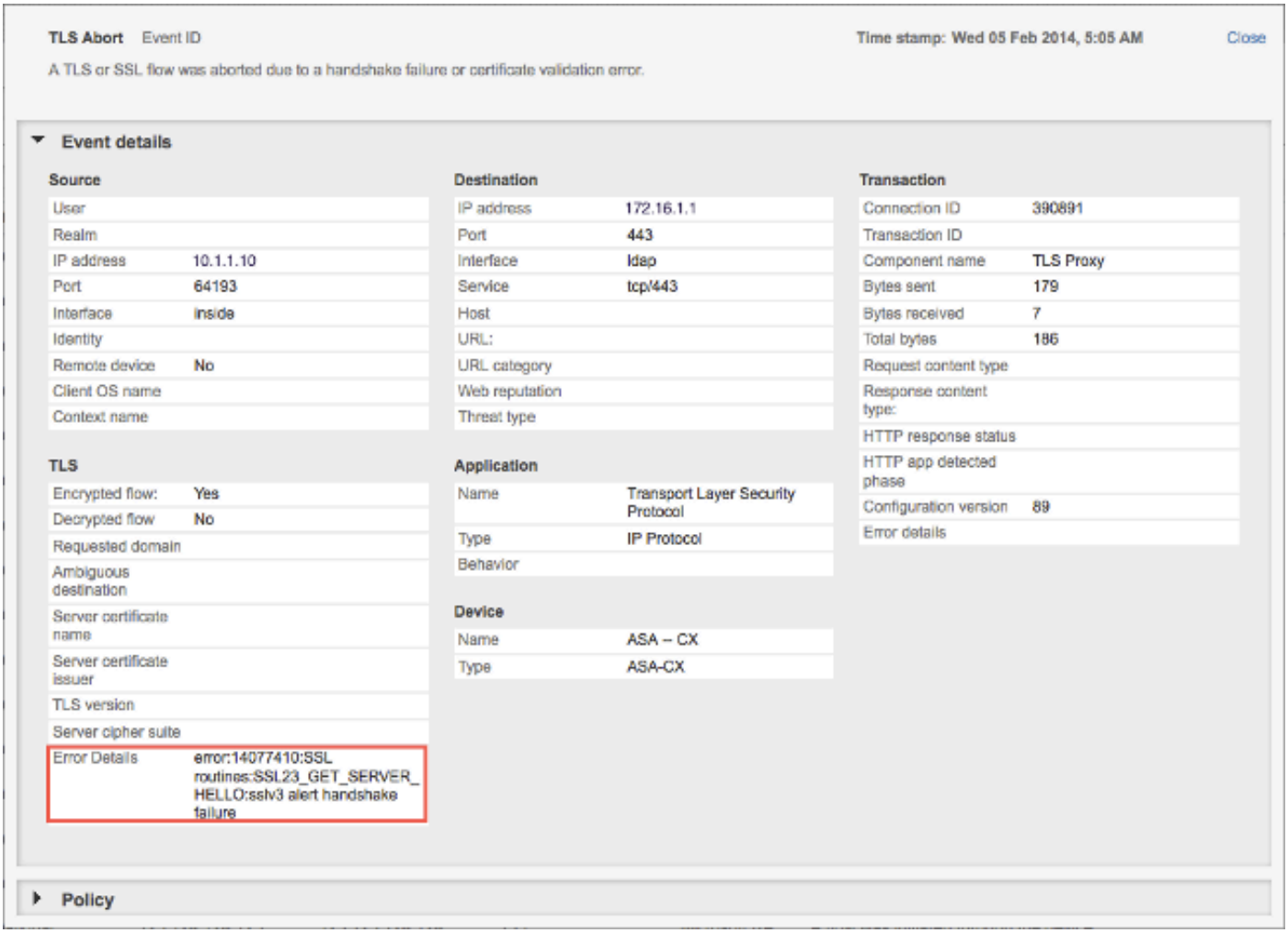
En esta imagen, **A** es el cliente, **B** es el módulo de servicios NGFW y **C** es el servidor HTTPS. Para los ejemplos proporcionados en este documento, el servidor basado en HTTPS es un Cisco Adaptive Security Device Manager (ASDM) en un Cisco Adaptive Security Appliance (ASA).

Hay dos factores importantes sobre este proceso que debe tener en cuenta:

- En el segundo paso del proceso, el servidor debe aceptar una de las suites de cifrado SSL que se presentan en el módulo de servicios de NGFW.
- En el cuarto paso del proceso, el módulo de servicios de NGFW debe confiar en el certificado que presenta el servidor.

Problema

Si el servidor no puede aceptar ninguno de los cifrados SSL presentados por el módulo de servicios NFGW, recibirá un mensaje de error similar a este:



Es importante tener en cuenta la información de detalles de error (resaltada), que muestra:

```
error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure
```

Cuando ve el archivo **/var/log/cisco/tls_proxy.log** en el archivo de diagnóstico del módulo, aparecen estos mensajes de error:

```
2014-02-05 05:21:42,189 INFO  TLS_Proxy   - SSL alert message received from
 server (0x228 = "fatal : handshake failure") in Session: x2fd1f6

2014-02-05 05:21:42,189 ERROR TLS_Proxy - TLS problem (error:14077410:
 SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure) while
 connecting to server for Session: x2fd1f6
```

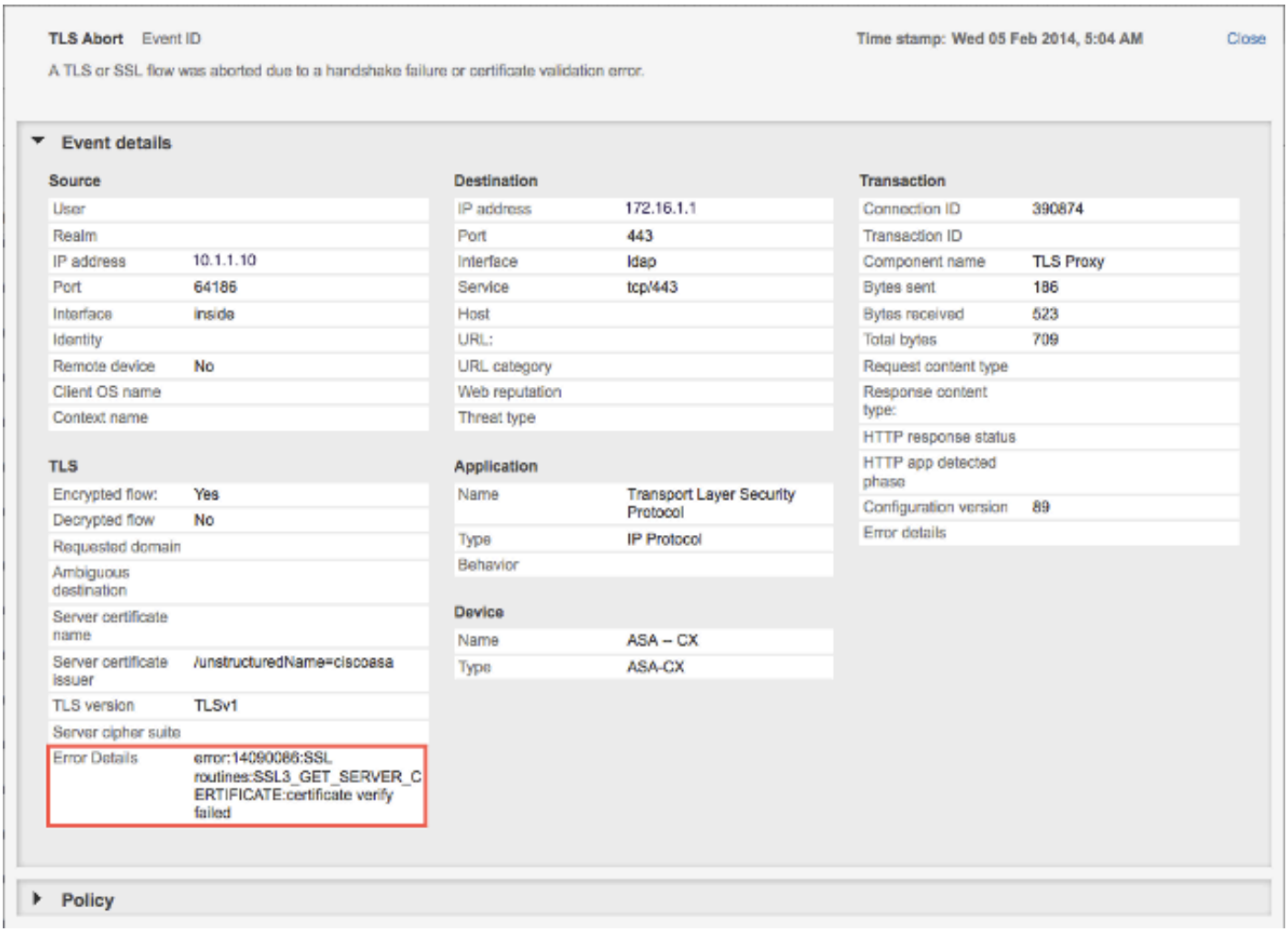
Solución

Una causa posible de este problema es que no se ha instalado en el módulo una licencia de triple estándar de cifrado de datos/estándar de cifrado avanzado (3DES/AES) (a menudo denominada K9). Puede descargar la licencia K9 para el módulo sin cargo y cargarla a través de PRSM.

Si el problema persiste después de instalar la licencia 3DES/AES, obtenga capturas de paquetes para el intercambio de señales SSL entre el módulo de servicios NGFW y el servidor, y póngase en contacto con el administrador del servidor para habilitar los códigos SSL apropiados en el servidor.

Problema

Si el módulo de servicios NGFW no confía en el certificado que presenta el servidor, recibirá un mensaje de error similar a este:



Es importante tener en cuenta la información de detalles de error (resaltada), que muestra:

```
error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
```

Cuando ve el archivo **/var/log/cisco/tls_proxy.log** en el archivo de diagnóstico del módulo, aparecen estos mensajes de error:

```
2014-02-05 05:22:11,505 INFO  TLS_Proxy - Certificate verification failure:
 self signed certificate (code 18, depth 0)

2014-02-05 05:22:11,505 INFO TLS_Proxy - Subject: /unstructuredName=ciscoasa

2014-02-05 05:22:11,505 INFO TLS_Proxy - Issuer: /unstructuredName=ciscoasa

2014-02-05 05:22:11,505 INFO TLS_Proxy - SSL alert message received from
 server (0x230 = "fatal : unknown CA") in Session: x148a696e

2014-02-05 05:22:11,505 ERROR TLS_Proxy - TLS problem (error:14090086:
 SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed) while
 connecting to server for Session: x148a696e
```

Solución

Si el módulo no puede confiar en el certificado SSL del servidor, debe importar el certificado del servidor en el módulo con PRSM para asegurarse de que el proceso de intercambio de señales SSL sea exitoso.

Complete estos pasos para importar el certificado del servidor:

1. Omita el módulo de servicios NGFW cuando accede al servidor para descargar el certificado a través de un navegador. Una manera de omitir el módulo es crear una política de descifrado que no descifra el tráfico a ese servidor en particular. Este vídeo muestra cómo crear la política:

   Estos son los pasos que se muestran en el vídeo:

   Para acceder al PRSM en el CX, navegue a **https://<IP_ADDRESS_OF_PRSM>**. Este ejemplo utiliza **https://10.106.44.101**.

   Vaya a **Configuraciones > Políticas/Configuración > Políticas de descifrado** en el PRSM.

   Haga clic en el icono que se encuentra cerca de la esquina superior izquierda de la pantalla y elija la opción **Agregar política anterior** para agregar una política a la parte superior de la lista.

   Asigne un nombre a la política, deje el origen como **Any** y cree un **objeto de grupo de red CX**.
   Nota: Recuerde incluir la dirección IP del servidor basado en HTTPS. En este ejemplo, se utiliza una dirección IP de **172.16.1.1**.Elija **No descifrar** para la acción.

   Guarde la política y realice los cambios.
2. Descargue el certificado del servidor a través de un navegador y cárguelo en el módulo de servicios NGFW a través de PRSM, como se muestra en este vídeo:

   Estos son los pasos que se muestran en el vídeo:

   Una vez definida la política mencionada anteriormente, utilice un navegador para navegar al servidor basado en HTTPS que se abre a través del módulo de servicios de NGFW.
   Nota: En este ejemplo, se utiliza Mozilla Firefox versión 26.0 para navegar al servidor (un ASDM en un ASA) con la URL **https://172.16.1.1**.Acepte la advertencia de seguridad si aparece y agrega una excepción de seguridad.

   Haga clic en el icono pequeño con forma de bloqueo situado a la izquierda de la barra de direcciones. La ubicación de este icono varía en función del explorador que se utiliza y de la versión.

   Haga clic en el botón **Ver certificado** y, a continuación, en el botón **Exportar** de la ficha

Detalles después de seleccionar el certificado del servidor.

Guarde el certificado en su equipo personal en el lugar que elija.

Inicie sesión en PRSM y busque **Configuraciones > Certificados**.

Haga clic en **I want to... > Importar certificado** y seleccionar el certificado de servidor previamente descargado (desde el paso 4).

Guarde y confirme los cambios. Una vez completado, el módulo de servicios NGFW debe confiar en el certificado que presenta el servidor.

3. Elimine la directiva que se agregó en el paso 1. El módulo de servicios NGFW ahora puede completar el intercambio de señales correctamente con el servidor.

Información Relacionada

- Guía del usuario para ASA CX y Cisco Prime Security Manager 9.2
- Soporte Técnico y Documentación - Cisco Systems